

UNITED STATES DISTRICT COURT

SEALED

for the
District of Nebraska

In the Matter of the Search of

(Briefly describe the property to be searched
or identify the person by name and address)

Information associated with the email address taylorleo576@gmail.com, that is stored at
premises owned, maintained, controlled, or operated by Google, Inc.,
1600 Amphitheatre Parkway Mountain View, CA 94043

Case No. 8:19MJ147

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____ California _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
21:841, 846

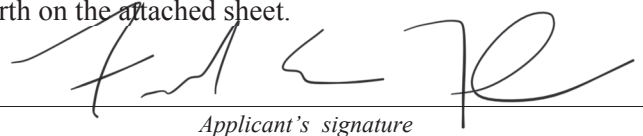
Offense Description

Conspiracy to distribute and possess with intent to distribute controlled substances

The application is based on these facts:

See affidavit

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.


Applicant's signature

☐ Sworn to before me and signed in my presence. SA Frank Feden, Drug Enforcement Administration

Printed name and title

- ☒ Sworn to before me by telephone or other reliable electronic means.


Judge's signature

Date: 3/26/2019

City and state: Omaha, Nebraska

Michael D. Nelson, U.S. Magistrate Judge

Printed name and title

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA**

IN THE MATTER OF THE SEARCH OF)
INFORMATION ASSOCIATED WITH) **Case No. 8:19MJ147**

taylorleo576@gmail.com)

STORED AT
Google, Inc.

FILED UNDER SEAL

AFFIDAVIT

I, Frank Feden, being first duly sworn, hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant for information associated with the email address taylorleo576@gmail.com, that is stored at premises owned, maintained, controlled, or operated by Google, Inc., an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) to require Google, Inc. to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with taylorleo576@gmail.com including the contents of communications.
2. I am a Special Agent (SA) with the United States Drug Enforcement Administration (DEA), and have been since May 2003, and I have graduated from the DEA Basic Agent Training in Quantico, Virginia. During my tenure as a Special Agent with the DEA, I have been assigned to investigations of violations of the drug laws of the United States including violations of Title 21, United States Code, Sections 841(a)(1) and Title 21, United States Code, Section 846.
3. In my work as a Special Agent with the DEA, I have been involved in controlled purchases, surveillance, electronic surveillance, arrest of drug traffickers, interviewing of drug traffickers, trash pulls, and the execution of search warrants on residences, businesses, vehicles and electronic devices. As a result, I have arrested individuals for violating State and Federal statutes regarding the possession, manufacture, transportation and sale of controlled substances. I have conducted and have been associated with investigations involving the interception of wire communications and electronic communications obtained from cellular telephone devices and smart phones. I am familiar with the ways in which drug traffickers conduct business, including, but not limited to, their methods of importing and distributing controlled substances, their use of cellular telephones, their use of computers and smart phones and their use of numerical codes and code words to conduct their transactions.

4. I am familiar with the facts and circumstances of this investigation through personal participation and from discussions with agents and officers involved in the investigation. I have also reviewed records and reports related to this investigation. Unless otherwise noted, wherever I assert that a statement was made, the information was provided by another agent, law enforcement officer or witness, who may have had either direct or hearsay knowledge of that statement, and to whom I, or others, have spoken, or whose reports I have read and reviewed. Such statements are among many statements made by others and are stated in substance and in part unless otherwise indicated. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included details of every aspect of the investigation. Facts not set forth herein, or in the attached exhibits, are not being relied upon in reaching the conclusion that the requested order should be issued. Nor do I request that this Court rely on any facts not set forth herein in reviewing this application.

PROBABLE CAUSE

5. In April 2018, DEA received a tip from Mallinckrodt Pharmaceuticals, a US company, that the company's morphine-sulfate pills were being advertised for sale on the website, silkroadmeds.com. The representative for Mallinckrodt Pharmaceuticals denied the company had a relationship with silkroadmeds.com, and the representative claimed that any product purported by silkroadmeds.com to be produced by Mallinckrodt Pharmaceuticals was more than likely a counterfeit product. Investigators visited silkroadmeds.com and observed that numerous brand name pharmaceutical drugs were listed for sale on the site. The site did not require customers to have a prescription to order controlled substances and it used Western Union and MoneyGram for customers to remit payment.

6. In April 2018, investigators accessed the website, "silkroadmeds.com", and using an undercover identity, placed an order for 60 Morphine-sulfate 30mg pills and 30 Oxycodone 40mg pills. Both Morphine-sulfate and Oxycodone are controlled substances and a valid prescription is required to purchase either in the United States. The price for the order was \$456.00 and a prescription was not required to place the order. The investigators received an email from sales@silkroadmeds.com directing them to send the payment for the order to Jamshaid MUSHTAQ in Lahore, Pakistan via Money Gram. The email also directed us to send an email to sales@silkroadmeds.com after the payment had been made.

7. The investigators completed the payment, and they confirmed that on May 2, 2018, Jamshaid MUSHTAQ presented a Pakistan Government issued identification card to a Money Gram Payment Systems Inc. Agent in Lahore, Pakistan prior to receiving the payment.

8. In May 2018, investigators received, via the undercover email account, an email from someone claiming to be Baritt LEE using email account busniesspluss@gmail.com. The email indicated that a package had been sent to our shipping address and the United States Postal System tracking number for that package was RR075512255PH. The email also indicated that the email was sent on behalf of the Silkroad Support Team. Using the provided tracking number, investigators tracked the package from Manila, Philippines to an undercover United States Post Office Box in Omaha, Nebraska.

9. The package, which was a small brown paper envelope addressed from Rabab MAMAILAO, Sucat Paranaque Manila, Philippines, 1700 09151692230, from the undercover Post Office Box. The package contained 50 small round blue pills with "M" imprinted on one side and "30" imprinted on the other side. From my training and experience, I recognized the pills to be Oxycodone 30mg pills manufactured by Mallinckrodt Pharmaceuticals. I then transferred the 50 pills to the DEA North Central Laboratory for analysis. The Forensic Chemist determined that the 50 pills did not contain Oxycodone but instead were made of Heroin, Caffeine, Acetaminophen, Methorphan and 06-Monoacetylmorphine. The pills had been pressed in a pill press to look like Oxycodone 30mg pills manufactured by Mallinckrodt Pharmaceuticals.

10. On June 26, 2018, Magistrate Judge Susan M. Bazis of the U.S. District Court, District of Nebraska issued a Search and Seizure Warrant for the email address busniesspluss@gmail.com. Investigators executed the warrant on June 27, 2018. On June 28, 2018, investigators received the data from Google Inc. with regards to the execution of the Search and Seizure Warrant for the email address busniesspluss@gmail.com.

11. The data provided by Google, Inc. for busniesspluss@gmail.com, listed rickpaul38@gmail.com as the accounts recovery e-mail. A Gmail recovery email address is an email address that clients of Gmail can list with the company so that if the client becomes locked out of their Gmail account they can have Google, Inc. reset the password and send that new password to them at the recovery e-mail. Google, Inc. also provided phone number 923470413699 as the number given to Google by the subscriber as a contact number. The busniesspluss@gmail.com contained over 25,000 emails with over 8,000 different email addresses. Almost all of the emails pertained to the sale of controlled prescription drugs inside and outside the United States, payment details and information for those drug sales and the shipping details and information for those drug sales. A review of the transactions disclosed that prescriptions were not provided to purchase controlled substances including all drugs shipped to the United States.

12. In July 2018, investigators conducted another online undercover purchase from silkroadmeds.com. The purchases occurred in the same manner as the first purchase. The investigators purchased 315 Oxycodone 30mg pills for \$1,950.75. A Chemist from DEA North Central Laboratory determined the pills were counterfeits and contained Heroin, Caffeine, Acetaminophen, Methorphan and 06-Monoacetylmorphine.

13. In August 2018, investigators learned from Google, Inc. that the subscriber listed for rickpaul38@gmail.com is Rick Paul and the contact phone for the account was 923470413699. That is the same phone number given to Google, Inc. by the user of busniesspluss@gmail.com.

14. On August 22, 2018, Magistrate Judge Bazis issued a Search and Seizure Warrant for the email address rickpaul38@gmail.com. Investigators executed the warrant on August 23, 2018. On September 5, 2018, investigators received the data from Google Inc. from the execution of the Search and Seizure Warrant for the email address rickpaul38@gmail.com.

15. The rickpaul38@gmail.com account contained 32,058 emails and the account had contact with over 8,000 different email addresses. The Gmail account received emails of drug orders

form the following websites: medscareonline.com, overallpharmacy.us, usrxmedsonline.com, overthcounter.com, overthcounter.org, overallpharmacy.com, usdrugsaver.com, us2us-rx.com, drugs-order.net, zampharma.com, drugsplace.com, oneplushealthcare.net, onlinerxhub.com, pillspharma.com, rxdrugpharmacy.com, legitrxshop.com, rxstuff.net, pharmadaddy.biz, rxpharmacyline.com, apexmedico.net, rxpharmaplus.net, uspharmacyhub.com, drugs-point.com and silkroadmeds.com. Each drug order was part of an email chain that showed the customers' initial orders to the websites. The email chain also showed how and when the customer paid for the drug order and when the website representative received the payment. The email chain would also show a tracking number for the package being sent to the customer. I found 17 email exchanges in regard to the customers claiming their orders had been seized by law enforcement and would the website resend the order at no cost.

16. During the search of the emails in rickpaul38@gmail.com account, investigators found over 500 emails pertaining to Nazmul HAQUE. Customers of the websites were directed to remit payments for drugs via Western Union and MoneyGram to Nazmul HAQUE in Florida. Customers were also given the option to wire the payment to Orine Beauty & Healthcare's Wells Fargo Bank Account of 6444404872. Orine Beauty & Healthcare is a business owned by HAQUE. Customers of the websites were also informed they could wire payments for drugs to Nazmul HAQUE's Wells Fargo Bank Account of 1010312205061. Finally, customers of the websites were also informed they could mail a check for payment to Nazmul HAQUE at 7099 Pine Manor Drive, Lake Worth, Florida 33467.

17. Investigators found a photograph of a check from a Jennifer JONES made payable to Nazmul HAQUE for \$220.00. Investigators also found emails where JONES ordered 60 Adderall 30mg pills from usrxmedsonline.com for a total cost of \$220.00.

18. Investigators learned that Mohammad Nazmul HAQUE was associated with the address of 7099 Pine Manor Drive, Lake Worth, Florida 33467 and with Orine Beauty & Healthcare. Investigators also learned that Wells Fargo Bank Account 1010312205061 is in Mohammad Nazmul HAQUE's name.

19. Investigators learned that on October 20, 2016, Special Agents with the United States Food and Drug Administration (FDA) interviewed HAQUE at his residence at 7099 Pine Manor Drive, Lake Worth, Florida. The FDA had received a complaint from a customer of ThePharmacyHub.com who had purchased Adderall, a controlled substance, from the website in 2015. The customer stated the Adderall was shipped from India and when the customer ingested the medicine they had an adverse reaction. The FDA later determined that the Adderall had actually been Tramadol, which is a controlled substance. ThePharmacyHub.com was registered with the State of Florida and HAQUE was listed as the registered owner. The customer used their credit card to pay for the drugs and the customer's credit card statement indicated the payment was made to Orine Beauty & Healthcare, which is a business registered to HAQUE with State of Florida.

20. During the interview with the investigators from the FDA, HAQUE denied he owned ThePharmacyHub.com. HAQUE stated his friend Ascef HASSEN, who lives in Pakistan, owns the business. HAQUE claimed that HASSEN used his identity without his permission to start the

online business. HAQUE admitted he agreed to process credit card payments for HASSEN using his Wells Fargo Bank account. HAQUE stated he only processed four or five credit cards for HASSEN. HAQUE admitted he would send the money from the processed credit cards to HASSEN in Pakistan. HAQUE claimed he learned HASSEN had registered ThePharmacyHub.com in HAQUE's name and HAQUE's email address when he received an email from a customer of the website claiming they had received the wrong drugs. HAQUE claimed he then stopped using his email and he told HASSEN to stop everything. HAQUE stated he and HASSEN are no longer friends.

21. In February 2019, investigators with DEA visited HAQUE's business website, Orinehealthcare.com, which sells vitamins and food supplements. The website also recruited individuals to fly luggage to Bangladesh for pay. The website listed the contact phone number for the business of 561-670-8276 and a contact email for the business of taylorleo576@gmail.com. Investigators further learned 561-670-8276 is a T-Mobile cellular phone subscribed to HAQUE.

22. On March 18, 2019, SA Matthew Kessler of the FDA and I contacted HAQUE at his residence at 1401 Village Boulevard Apartment 813, West Palm Beach, Florida and he agreed to speak to me and SA Kessler. During the interview, HAQUE admitted he conducted numerous credit card transactions for customers of some of the websites listed in paragraph 15 of this affidavit and he admitted he received money wires from those websites' customers via MoneyGram or Western Union. HAQUE also admitted he received checks from those websites' customers and deposited them into his Wells Fargo Bank accounts. HAQUE claimed he did not know the payments he accepted were for drugs and he thought the payments were for medicines. HAQUE stated he withdrew the money from his bank accounts and he wired the money as directed by his business associate in Lahore, Pakistan via MoneyGram and or Western Union.

23. HAQUE stated he did not know his business associate's name and he knew him only as "brother". HAQUE stated numerous members of his business associate's family were involved with the websites that sold medicines and he knew the medicines were shipped from the Philippines, India, Pakistan and Spain. HAQUE stated he spoke to his business associate a few times using WhatsApp and his business associate's number was 92-3086240729. HAQUE stated he sent and received text messages via WhatsApp to and from 92-3086240729. HAQUE stated most of his communications with his business associate were by email. HAQUE stated he used his Gmail account of taylorleo576@gmail.com to send and receive most of his emails with his business associate. HAQUE stated he did not steal Leo TAYLOR's identity and it was just a name he made up that he occasionally uses instead of his own.

24. On March 19, 2019, I spoke with Kristina Nickols, who had been an employee of HAQUE's in 2013 and 2014. Nickols stated in October 2014, HAQUE asked her if he could use her PayPal account. HAQUE told her he had business associates, whose customers wanted to pay via PayPal. Nickols agreed to HAQUE's request, and a few days after he processed the transactions, she received an email from PayPal notifying her that her PayPal account had been suspended for violation of PayPal's ban on selling prescription drugs. Additionally, Nickols stated HAQUE had transferred the funds received from the transaction to another account and he transferred \$137.00 more than what her account received, which left her account with a negative balance. Nickols stated she confronted HAQUE and showed him the email from PayPal. She

stated HAQUE told her he would speak with his business associates and would get her money back. Nickols stated HAQUE never repaid her and she quit working for him before the end of 2014. Investigators learned from PayPal that the funds from the transaction were transferred from Nickols PayPal account to Leo TAYLOR's PayPal account. The funds were then transferred to a Wells Fargo Bank account held by HAQUE. Leo TAYLOR's PayPal account listed a contact number of 561-670-8276, which is HAQUE's cell phone number.

25. From the evidence contained in the seized email from rickpaul38@gmail.com in regard to HAQUE receiving and processing payments for drug purchases and from HAQUE's statement about his involvement with his business associate in Pakistan scheme, I believe HAQUE participated in violations of 21 USC 841 and 21 USC 846 and evidence of his participation is contained on his Gmail account of taylorleo576@gmail.com.

ADDITIONAL INFORMATION

26. Google, Inc. provides a variety of on-line services, including email access, to the general public. Google, Inc. allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with Google, Inc. During the registration process, Google, Inc. asks subscribers to provide basic personal information. Therefore, the computers of Google, Inc. are likely to contain stored electronic communications (including retrieved and unretrieved email for Google, Inc. subscribers) and information concerning subscribers and their use of Google, Inc. services, such as account access information, email transaction information, and account application information.

27. In general, an email that is sent to a Google, Inc. subscriber is stored in the subscriber's "mail box" on Google, Inc. computer systems until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google, Inc. computer systems indefinitely. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Google, Inc.'s computer systems, and then transmitted to its end destination. Google, Inc. often saves a copy of the email sent. Unless the sender of the email specifically deletes the email from the Google, Inc. computer system, the email can remain on the system indefinitely. Even if the sender deletes the e-mail, it may continue to be available on Google's servers for a certain period of time. A sent or received email typically includes the content of the message, source and destination addresses, the date and time at which the email was sent, and the size and length of the email. If an email user writes a draft message but does not send it, that message may also be saved by Google, Inc. but may not include all of these categories of data.

28. A Google, Inc. subscriber can also store files, including emails, address books, contact or buddy lists, calendar data, pictures, and other files, on computer systems maintained and/or owned by Google, Inc.

29. Subscribers to Google, Inc. might not store on their home computers copies of the

emails stored in their Google, Inc. account. This is particularly true when they access their Google, Inc. account through the web, or if they do not wish to maintain particular emails or files in their residence.

30. In general, email providers like Google, Inc. ask each of their subscribers to provide certain personal identifying information when registering for an email account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

31. Email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of login (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google, Inc.'s website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

32. In some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

33. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

34. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A), by using the warrant to require Google, Inc. to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

35. Based on the provided information, there is probable cause to believe taylorleo576@gmail.com account contains evidence of violations of Title 21, United States Code §§ 841, 846 and other violations of federal code.

36. Based on the forgoing, I request that the court issue the proposed search warrant. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction: as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the court is "a district court of the United States ... that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING AND ORDER UNDER 18 U.S.C. § 2705

37. The investigation of the criminal activity discussed above is ongoing and may involve multiple targets, many of whom may not have yet been identified. Moreover, the DEA is not aware of any potential targets that have knowledge of its investigation. Disclosure of the search warrant, this affidavit, or this application may result in the dissemination of these materials to the targets, who may destroy evidence or otherwise evade the investigation. Disclosure of the contents of this affidavit and related documents might have a significant and negative impact on the continuing investigation and might severely jeopardize its effectiveness. Accordingly, I respectfully request that the Court issue an order that the search warrant, this affidavit in support of the application for the search warrant, and the application for the search warrant be filed under seal until further order of this Court. Although the above documents may be sealed, it is respectfully requested that the data obtained as a result of the search warrant may be disclosed to third parties to facilitate analysis. I further request that the Court issue an order commanding Google, Inc, not notify any person of the existence of the search warrant under 18 U.S.C. § 2705(b).

CONCLUSION

38. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that HAQUE using the account taylorleo576@gmail.com violated 21 U.S.C. § 841 (Distribution of a Controlled Substance) and § 846 (Conspiracy to Distribute a Controlled Substance). There is also probable cause that evidence of these crimes will be found in the account of taylorleo576@gmail.com.

A handwritten signature in black ink, appearing to read 'Frank E. Feden', written over a horizontal line.

FRANK E. FEDEN
Special Agent
US Drug Enforcement Administration

Sworn to before me by reliable electronic means:

Date: 03/26/2019

City and State: Omaha, Nebraska

A handwritten signature in black ink, appearing to read 'Michael D. Nelson', written over a horizontal line.

Michael D. Nelson, U.S. Magistrate Judge

ATTACHMENT A

Property to be searched

This warrant applies to information associated with taylorleo576@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B

Items to be Seized

I. Information to be disclosed by Google Inc.

This search warrant will be e-mailed or faxed to Google personnel by law enforcement agents. Google personnel are directed to isolate and disclose to the government the account and files described below related to the email accounts:

- taylorleo576@gmail.com for the period from the creation of the account to the date of this search warrant

1. All electronic mail stored and presently contained in, or on behalf of, the above email accounts, for the above specified periods.

2. All transactional information, session times and durations, content and connection log files of all activity for the above specified periods, by the users associated with the above referenced email account, including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable / DSL, T1 / LAN), ports used, telephone dial-up caller identification records, any other connection information or traffic data and records of the originating Internet Protocol Addresses of the user when he connected to Google.

3. All business records and subscriber information, in any form kept, pertaining to the above referenced email account, including applications, subscribers' full names, all screen names associated with the subscribers and/or email account, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, detailed billing records, types and lengths of service, and any other identifying information.

4. All instant messages stored and presently contained in, or on behalf of, the above referenced email account for the above specified periods.

5. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, location and direction information, files and data involved in the administration and management of websites, and other stored documents, notes, spread sheets and files.

6. All records and data related to mobile phones linked to, or accessing, the account, to include the unique identifiers such as IMEI numbers and contents of any mobile phone backups found within the account.

In order to minimize any disruption of computer service to innocent third parties, Google employees will create an exact duplicate of the computer accounts and files described above, including an exact duplicate of all information stored in the computer account and files described therein. Google employees will then provide the exact duplicate of the account and files described above and all information stored in those accounts and files to law enforcement agents, who need not be present during the duplication of the files, in electronic form not later than 7 days from the date of this search warrant.

II. Information to be seized by law enforcement as evidence

Law enforcement personnel will thereafter review the information and files received from Google related to the email accounts:

- taylorleo576@gmail.com for the period from the creation of the account to the date of this search warrant

and then identify, copy and seize any evidence of violations of 21 U.S.C. §841 and 21 U.S.C. §846 including the following, all of which constitutes evidence:

1. Emails relating to the unauthorized importation, distribution, manufacture and sale of controlled substance or pharmaceutical drugs for the above specified period of time for the specified email account, including, without limitation, email communications (including email attachments) that are records of, or relate to:

a) the mailing, transportation, ordering, purchasing, receipt, manufacture, importation and/or distribution of controlled substance or pharmaceutical drugs:

b) financial transactions for the obtaining, secreting, transferring, importation and concealment of controlled substance or pharmaceutical drugs:

c) financial transactions evidencing expenditure of money made from engaging in illegal controlled substance or pharmaceutical drugs trafficking activity in, and/or importation of controlled substance or pharmaceutical drugs:

d) the ownership of assets obtained from illegal importation of, and/or trafficking controlled substance or pharmaceutical drugs:

e) Records of telephone numbers, address books, or papers which reflect names, addresses, and/or telephone numbers of associates and co-conspirators involved directly and indirectly in the smuggling and/or trafficking in controlled substance or pharmaceutical drugs and/or associates who have a monetary consideration and/or interest in the illegal smuggling or trafficking of controlled substance or pharmaceutical drugs: and

f) Correspondence that reflects the importation, trafficking, distribution, manufacture and/or mailing of controlled substances or pharmaceutical drugs:

2. All transactional information, session times and durations, content and connection log files of all activity for the above specified periods, by the users associated with the above referenced email accounts, including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable/DSL, T1/LAN), ports used, telephone dial-up caller identification records, any other connection information or traffic data and records of the originating Internet Protocol Addresses of the user when he connected to Google.

3. All business records and subscriber information, in any form kept, pertaining to the above referenced email accounts, including applications, subscribers' full names, all screen names associated with the subscribers and/or email accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, detailed billing records, types and lengths of service, and any other identifying information.

4. All instant messages stored and presently contained in, or on behalf of, the above referenced email accounts for the above specified period reflecting the importation, trafficking, distribution, manufacture and/or mailing of controlled substance or pharmaceutical drugs; and/or the handling of proceeds and assets obtained therefrom.

UNITED STATES DISTRICT COURT

SEALEDfor the
District of Nebraska

In the Matter of the Search of

Information associated with the email address
taylorleo576@gmail.com, that is stored at premises owned,
maintained, controlled, or operated by Google, Inc.,
1600 Amphitheatre Parkway Mountain View, CA 94043

Case No. 8:19MJ147

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search
of the following person or property located in the _____ District of _____ California
(identify the person or describe the property to be searched and give its location):

SEE ATTACHMENT A (INCORPORATED BY REFERENCE)

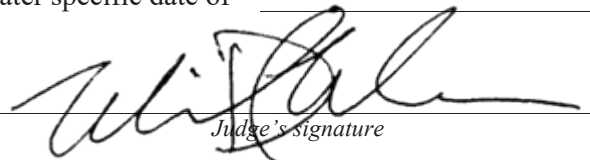
I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property
described above, and that such search will reveal (identify the person or describe the property to be seized):

SEE ATTACHMENT B (INCORPORATED BY REFERENCE)

YOU ARE COMMANDED to execute this warrant on or before April 9, 2019 (not to exceed 14 days)☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the
person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the
property was taken.The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory
as required by law and promptly return this warrant and inventory to Michael D. Nelson
(United States Magistrate Judge)☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C.
§ 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose
property, will be searched or seized (check the appropriate box)☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____

Date and time issued: March 26, 2019, 1:03 p.m.

City and state: Omaha, Nebraska


Judge's signatureMichael D. Nelson, U.S. Magistrate Judge
Printed name and title

AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

ReturnCase No.:
8:19MJ147

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

Property to be searched

This warrant applies to information associated with taylorleo576@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google, Inc., a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043.

ATTACHMENT B

Items to be Seized

I. Information to be disclosed by Google Inc.

This search warrant will be e-mailed or faxed to Google personnel by law enforcement agents. Google personnel are directed to isolate and disclose to the government the account and files described below related to the email accounts:

- taylorleo576@gmail.com for the period from the creation of the account to the date of this search warrant

1. All electronic mail stored and presently contained in, or on behalf of, the above email accounts, for the above specified periods.

2. All transactional information, session times and durations, content and connection log files of all activity for the above specified periods, by the users associated with the above referenced email account, including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable / DSL, T1 / LAN), ports used, telephone dial-up caller identification records, any other connection information or traffic data and records of the originating Internet Protocol Addresses of the user when he connected to Google.

3. All business records and subscriber information, in any form kept, pertaining to the above referenced email account, including applications, subscribers' full names, all screen names associated with the subscribers and/or email account, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, detailed billing records, types and lengths of service, and any other identifying information.

4. All instant messages stored and presently contained in, or on behalf of, the above referenced email account for the above specified periods.

5. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, location and direction information, files and data involved in the administration and management of websites, and other stored documents, notes, spread sheets and files.

6. All records and data related to mobile phones linked to, or accessing, the account, to include the unique identifiers such as IMEI numbers and contents of any mobile phone backups found within the account.

In order to minimize any disruption of computer service to innocent third parties, Google employees will create an exact duplicate of the computer accounts and files described above, including an exact duplicate of all information stored in the computer account and files described therein. Google employees will then provide the exact duplicate of the account and files described above and all information stored in those accounts and files to law enforcement agents, who need not be present during the duplication of the files, in electronic form not later than 7 days from the date of this search warrant.

II. Information to be seized by law enforcement as evidence

Law enforcement personnel will thereafter review the information and files received from Google related to the email accounts:

- taylorleo576@gmail.com for the period from the creation of the account to the date of this search warrant

and then identify, copy and seize any evidence of violations of 21 U.S.C. §841 and 21 U.S.C. §846 including the following, all of which constitutes evidence:

1. Emails relating to the unauthorized importation, distribution, manufacture and sale of controlled substance or pharmaceutical drugs for the above specified period of time for the specified email account, including, without limitation, email communications (including email attachments) that are records of, or relate to:

a) the mailing, transportation, ordering, purchasing, receipt, manufacture, importation and/or distribution of controlled substance or pharmaceutical drugs:

b) financial transactions for the obtaining, secreting, transferring, importation and concealment of controlled substance or pharmaceutical drugs:

c) financial transactions evidencing expenditure of money made from engaging in illegal controlled substance or pharmaceutical drugs trafficking activity in, and/or importation of controlled substance or pharmaceutical drugs:

d) the ownership of assets obtained from illegal importation of, and/or trafficking controlled substance or pharmaceutical drugs:

e) Records of telephone numbers, address books, or papers which reflect names, addresses, and/or telephone numbers of associates and co-conspirators involved directly and indirectly in the smuggling and/or trafficking in controlled substance or pharmaceutical drugs and/or associates who have a monetary consideration and/or interest in the illegal smuggling or trafficking of controlled substance or pharmaceutical drugs: and

f) Correspondence that reflects the importation, trafficking, distribution, manufacture and/or mailing of controlled substances:

2. All transactional information, session times and durations, content and connection log files of all activity for the above specified periods, by the users associated with the above referenced email accounts, including dates, times, methods of connecting (e.g., telnet, ftp, http), type of connection (e.g., modem, cable/DSL, T1/LAN), ports used, telephone dial-up caller identification records, any other connection information or traffic data and records of the originating Internet Protocol Addresses of the user when he connected to Google.

3. All business records and subscriber information, in any form kept, pertaining to the above referenced email accounts, including applications, subscribers' full names, all screen names associated with the subscribers and/or email accounts, all account names associated with the subscribers, methods of payment, telephone numbers, addresses, passwords, detailed billing records, types and lengths of service, and any other identifying information.

4. All instant messages stored and presently contained in, or on behalf of, the above referenced email accounts for the above specified period reflecting the importation, trafficking, distribution, manufacture and/or mailing of controlled substance or pharmaceutical drugs; and/or the handling of proceeds and assets obtained therefrom.